UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

MICHELLE DAVIS, on behalf of herself and all others similarly situated, Plaintiff, v. NUANCE COMMUNICATIONS, INC. and GEISINGER HEALTH, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Michelle Davis ("Plaintiff") brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendants, NUANCE COMMUNICATIONS, INC. and GEISINGER HEALTH ("Defendants"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") and protected health information ("PHI") owe a duty to the individuals to whom that data relates, including patients and employees. This duty arises based upon the parties' relationship and because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

3. As a healthcare provider and vendor for a healthcare provider, Defendants are required by law to provide every patient with a Notice of Privacy Practices.

4. Defendants knowingly obtain patient's PII and PHI and has a resulting duty to securely maintain such information in confidence.

5. Plaintiff brings this class action on behalf of individuals and patients of Defendants, or otherwise people that are customers of or have their records collected by Defendants, whose PII and/or PHI was accessed and exposed to unauthorized third parties during a data breach that was first announced by Defendants in June of 2024 (the "Data Breach").

6. On or about November 29, 2023, Defendant Geisinger discovered that a former Nuance employee had accessed and obtained the PII and/or PHI of Plaintiff and other class members.

7. Despite the fact that Defendants became aware of the Data Breach on November 29, 2023, they failed to notify the Plaintiff and the putative Class Members until June 2024.

8. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty/confidence, breach of implied contract, unjust enrichment, and declaratory judgment, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Defendants to date, a wide variety of PII and PHI was implicated in the breach. This includes the following: names, dates of birth, addresses, medical record numbers, race, gender, admit and discharge or transfer codes, phone numbers, and facility name abbreviations.

10. As a direct and proximate result of Defendants' inadequate data security, their breach of duty to handle PII and PHI with reasonable care, and their failure to maintain the confidentiality of patients' medical records and PHI, Plaintiff's and Class Members' PII and/or PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

11. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

12. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, along with declaratory judgment and injunctive relief requiring Defendant to, at minimum: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

13. Plaintiff Michelle Davis is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff's PHI and PII records were maintained within Defendants' networks, as Plaintiff received healthcare services from Defendant Geisigner. Shortly after June 21, 2024, Plaintiff received a notice letter from Defendant informing Plaintiff that her PII and PHI may have been accessed or exposed to unknown, unauthorized third parties during the Data Breach, including but not limited to her name, date of birth, address, medical record number, race, gender, admit and discharge or

transfer code, phone number and facility name abbreviation.

14. Defendant Nuance Communications, Inc. ("Nuance") is a Delaware corporation with its principal place of business at 1 Wayside Road, Burlington, Massachusetts 01803. Nuance is a provider of healthcare information technology services and is a third party vendor for Defendant Geisinger. Nuance may be served at its registered agent, Corporation Service Company located at 84 State Street, Boston, Massachusetts, 02109

15. Defendant Geisinger Health ("Geisinger") is a Pennsylvania nonprofit corporation with its principal place of business located at 100 North Academy Avenue, Danville, Pennsylvania 17822. Geisinger is a healthcare provider serving various communities in Pennsylvania.

JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over this nationwide class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A). The Court has personal jurisdiction over Defendants because they own and operate businesses that are located and headquartered in Pennsylvania and conduct substantial business throughout Pennsylvania.

17. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the acts giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

18. At all relevant times, Defendants knew they were storing and permitting their employees to use internal network servers to transmit valuable, sensitive PII and PHI and that, as a result, Defendants' systems would be attractive targets for criminals and/or cybercriminals.

19. Defendants also knew that any breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

20. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others. Healthcare companies have been targeted most recently including the Kaiser Foundation Health Plan, HCA Healthcare, and Managed Care of North America (MCNA Dental), to name a few.

21. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

22. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the IRTC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-

[1] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

sensitive" records.[2]

23. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[3]

24. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[4]

25. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[5]

26. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

27. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up

---

[2] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[3] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

[4] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

[5] *Id.*

to—we've even seen $60 or $70."[6] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[7]

28. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[8]

29. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[9]

---

[6] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[7] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com /gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[8] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[9] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

30. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[10]

31. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its PII and PHI

32. On November 29, 2023, Geisinger discovered that a former Nuance employee had accessed certain Geisinger patient information two days after the employee had been terminated.

33. Nuance failed to revoke the employee's access to confidential patient information after the employee was terminated. After being notified by Geisinger of the Data Breach, Nuance permanently disconnected its former employee's access to Geisinger's records.

34. According to Defendants, they conducted an investigation and determined that personal information of patients was affected by the Data Breach.

---

[10] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

35. All in all, more than 1.2 million individuals may have had their PII and/or PHI breached.

36. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures, and their failure to follow their own policies, in order to protect its patients' PII and PHI.

37. Plaintiff received the notice from Defendant Nuance dated June 21, 2024, advising that Plaintiff was a victim of Defendants' data security failures exposing PHI and PII. A copy of the Notice is attached as Exhibit A.

38. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

39. In its notice to Plaintiff and Class members, Defendant asserted: "[t]he security of your personal information is very important to us." The notice further stated: "[w]e deeply regret any inconvenience or concern this may cause you."

40. The notice letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendants completed their investigation, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendants know if the data has been further disseminated.

41. Defendants Nuance acknowledges that it is responsible to safeguard Plaintiff and Class Members' PHI and PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PHI and PII.

42. Patients who receive healthcare services, such as Plaintiff, entrusted their PHI and PII to Defendants with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff and Class Members' PHI and PII from disclosure.

44. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Nuance and Geisinger to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

45. Defendants were well aware that the PHI and PII they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

46. The ramifications of Defendant's failure to keep PHI and PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

47. Further, criminals often trade stolen PHI and PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI and PII on the internet, thereby making such information publicly available.

48. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go

---

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 2, 2023).

undetected until debt collection calls commence months, or even years, later.[12] This time lag between when harm occurs versus when it is discovered, and also between when PHI and PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

49. Defendants knew, or should have known, the importance of safeguarding PHI and PII entrusted to them and of the foreseeable consequences if their systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

50. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI and/or PII.

51. Despite all of the publicly available knowledge of the continued compromises of PHI and PII, Nuance's and Geisinger's approach to maintaining the privacy of the PHI and PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

52. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendants' misfeasance.

53. Once PHI and PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

---

[12] *Identity Theft and Your Social Security Number*, Social Security Administrative, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 2, 2023).

54. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

55. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;
b. Unauthorized use and misuse of their PII and/or PHI;
c. The loss of the opportunity to control how their PII and/or PHI is used;
d. The diminution in value of their PII and/or PHI;
e. The compromise, publication, and/or theft of their PII and/or PHI;
f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
h. Costs associated with placing freezes on credit reports;
i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;
j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
k. The continued risk to their PII and/or PHI, which remains in the possession of Defendants and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII and/or PHI in their possession; and

l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

56. To date, Defendants have not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, they has taken to secure the PHI and PII still in their possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Defendants have proper measures in place to prevent another breach from occurring in the future.

57. Defendants were expressly prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

58. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[13]

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[14] The guidelines note that businesses should protect the personal customer information that they keep; properly

---

[13] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed June 2, 2023).

[14] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 2, 2023).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. Defendants failed to properly implement basic data security practices. Their failure to employ reasonable and appropriate measures to protect against unauthorized access to PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

62. Defendants were at all times fully aware of their obligation to protect PHI and PII and were also aware of the significant repercussions that would result from their failure to do so.

C. Plaintiff and Class Members Suffered Damages

63. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

64. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

65. As a result of Defendants' failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

66. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[15]

67. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[16]

68. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[17]

69. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[18]

---

[15] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[16] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[17] *Id.*

[18] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

70. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[19]

71. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[20]

72. Plaintiff and the Class members have also been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PHI.

73. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their patients' PII and PHI.

CLASS ALLEGATIONS

74. Plaintiff bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following classes:

> **Nationwide Class**
> All individuals in the United States whose PII and/or PHI was maintained by the Defendants and who were sent a notice of the Data Breach.
>
> **Pennsylvania Sub Class**
> All individuals in Pennsylvania whose PII and/or PHI was maintained by the Defendants and who were sent a notice of the Data Breach.

---

[19] *Id.*

[20] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

75. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

76. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

77. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Based on public information, the Class includes over 1.2 million individuals.

78. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants had a duty to maintain the confidentiality of Plaintiff and Class Members' PHI;

c. Whether Defendants breached their obligation to maintain Plaintiff and the Class members' medical information in confidence;

d. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached their duties thereby;

e. Whether Defendants breached their fiduciary duty to Plaintiff and the Class.

f. Whether Defendants failed to properly give notice under relevant law;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

h. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendants' wrongful conduct; and

i. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

79. **Typicality**. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendants to safeguard PII and PHI. Plaintiff and Class Members all entrusted their PII and PHI to Defendants, and each of them had their PII and PHI obtained by an unauthorized third party.

80. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

81. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached

their common law and statutory duties to secure PII and PHI on their network servers, then Plaintiff and each Class Member suffered damages from the exposure of their sensitive personal information in the Data Breach.

82. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

83. **Manageability.** While the precise size of the Class is unknown without the disclosure of Defendants' records, public records indicate at least 1.2 million individuals whose PII and/or PHI was compromised in the Data Breach. The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE and NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

84. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

85. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

86. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

87. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

88. Defendants' duty also arose from Defendants' position as a provider of healthcare and a third-party vendor. Defendants hold themselves out as trusted providers of healthcare and information technology services, and thereby assume a duty to reasonably protect their patients' information. Indeed, Defendants were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

89. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust i their ts information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow their own privacy policies and practices published to their patients.

90. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

91. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

92. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of their patients.

93. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

94. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

95. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act was intended to guard against.

96. Pursuant to Defendant Nuance's website, it acknowledged its legal duties by stating the following:

a) "HIPAA requires that covered entities and their business associates apply administrative, technical, and physical safeguards to maintain the confidentiality, integrity, and availability of electronic-protected health information (ePHI)."[21]

b) "An essential aspect of the benefits that we offer is our approach to processing personal information and sensitive or special category data. We believe it is critical to protect this information and to use it safely, securely, responsibly, and

[21] *See* https://www.nuance.com/about-us/trust-center/privacy/hipaa.html (last visited July 11, 2024).

proportionally. At Nuance, we are committed to safeguarding the personal information and the data we hold. We employ sophisticated data handling methods to guard an individual's privacy while ensuring that the data remains useful for the purpose and support that people require."[22]

c) "Nuance operates in a diverse and dynamic legal landscape. As a global company, we monitor evolving worldwide privacy and data protection laws and regulations and are firmly committed to meeting or exceeding new requirements that apply to our business."[23]

d) "Recent privacy legislation and legal decisions . . . have impacted companies and organizations worldwide, making it clear that additional supplemental measures are needed when processing or transferring personal data. We evaluated the protocols we rely on to protect personal data, including encryption, de-identification, pseudonymization, masking, and other measures, to ensure that such protocols align with evolving legal requirements."[24]

e) "We follow generally accepted standards to protect the personal data submitted to us, both during transmission and once it is received. Information you provide to us is stored on our secure servers."[25]

f) "Our Cyber Fusion Center (CFC) takes preventative and proactive measures to protect our networks, systems, and data from threats while adhering to security policies, standards, and controls across our infrastructure."[26]

---

[22] *See* https://www.nuance.com/about-us/trust-center/privacy/de-identification-pseudonymization.html (last visited July 11, 2024).
[23] *See id.*
[24] *See id.*
[25] *See* https://www.nuance.com/about-us/company-policies/privacy-policies.html (last visited July 11, 2024).
[26] *See* https://www.nuance.com/about-us/trust-center/security.html (last visited July 11, 2024).

g) "There are many laws that require that personally identifiable information be kept securely and only be used within certain parameters. . . . All of these confidentiality requirements remain in place even after an employee leaves Nuance."[27]

h) "Nuance is committed to responsibly handling the information entrusted to us. We have an obligation to protect the privacy of the personal information we hold."[28]

i) "Nuance is committed to complying with all laws, rules, and regulations that apply to us or our customers."[29]

97. Pursuant to Defendant Geisinger's website, it acknowledged its legal duties by stating the following:

a) "Under HIPAA, the information Geisinger collects about you as a patient is generally considered protected health information (PHI). Geisinger may only use and disclose your PHI pursuant to an authorization, or as otherwise permitted or required by law."[30]

b) "Pennsylvania law may further limit how we use or share your PHI including HIV-related records, records of alcohol or substance use disorder, inpatient mental health records and involuntary outpatient mental health treatment records. If Pennsylvania law applies to your PHI, we will use and disclose your PHI in compliance with these more restrictive laws."[31]

---

[27] *See* https://www.nuance.com/asset/en_us/collateral/corporate/company-policies/cp-nuance-code-of-conduct-june-2023.pdf (last visited July 11, 2024).
[28] *See id.*
[29] *See id.*
[30] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs (last visited July 11, 2024).
[31] *See id.*

c) "We are required by law to maintain the privacy and security of your PHI. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information. This will be done by mail or by other means if necessary."[32]

d) "We are subject to the United States laws and regulations that govern the privacy and security of patient healthcare information, as well as consumer protection laws and regulations of the United States and its individual states, as applicable."[33]

e) "Geisinger is committed to protecting the privacy and confidentiality of its patients' and members' medical information."[34]

f) "As a healthcare organization, Geisinger collects personal information about you as a patient or health plan member. In fact, we're often required to do so. The data we collect is key to our mission as a learning health system: to deliver the best and safest care, to advance medicine and healthcare delivery and to educate future healthcare professionals. We have an ethical obligation to use data responsibly. That's why we're transparent about how we use and share your data to support our missions — while protecting your privacy and interests."[35]

g) "We comply with all applicable federal and state laws and follow best practices to protect your data against loss, theft, unauthorized access, use, modification or disclosure. We train our staff and monitor their performance in keeping your data

---

[32] *See id.*
[33] *See id.*
[34] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa (last visited July 11, 2024).
[35] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/geisingers-principles-for-the-ethical-use-of-data (last visited July 11, 2024).

secure."[36]

98. Defendants violated their own policies by actively disclosing Plaintiff's and the Class Members' PII and/or PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and/or PHI; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of PII and/or PHI to Plaintiff and the Class.

99. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the

[36] *See id.*

hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PII and/or PHI;

j. The erosion of the essential and confidential relationship between Defendants – as a health care services provider – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

100. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Classes)

101. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

102. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendants and that

was ultimately accessed or compromised in the Data Breach.

103. As a healthcare provider, Defendants have a fiduciary relationship to their patients, like Plaintiff and the Class Members.

104. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII and PHI related to Plaintiff and the Class, which they were required to maintain in confidence.

105. Defendants owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

106. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the information within Plaintiff and the Class members' medical records.

107. Patients like Plaintiff and Class members have a privacy interest in personal medical matters, and Defendants had a fiduciary duty not to disclose medical data concerning patients.

108. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII and PHI of Plaintiff and Class members, information not generally known.

109. Plaintiff and Class Members did not consent to nor authorize Defendants to release or disclose their PHI to an unknown criminal actor.

110. Defendants breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data

security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security programs in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their patients and customers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class members' PHI and medical records/information to a criminal third party.

111. But for Defendants' wrongful breach of their fiduciary duties owed to Plaintiff and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

112. As a direct and proximate result of Defendants' breach of their fiduciary duties and breach of their confidences, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendants – as a health care services providers – and Plaintiff and Class members as patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendants.

113. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

114. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

115. When Plaintiff and members of the Class provided their personal information to Defendants, Plaintiff and members of the Class entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

116. Defendants required Plaintiff and class members to provide and entrust their PHI and PII and financial information as a condition of obtaining Defendants' services.

117. Plaintiff and Class members would not have provided and entrusted their PHI and PII and financial information to Defendants in the absence of the implied contract between them and Defendants.

118. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendants.

119. Defendants breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

120. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

121. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

122. This count is brought in the alternative to Plaintiff's breach of contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

123. Plaintiff and Class members conferred a benefit on Defendants by way of customers' paying Defendants to maintain Plaintiff and Class members' personal information.

124. The monies paid to Defendants were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

125. Defendants failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result Defendants were overpaid.

126. Under principles of equity and good conscience, Defendants should not be permitted to retain the money because Defendants failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

127. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

128. Defendants' enrichment at the expense of Plaintiff and Class members is and was unjust.

129. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

130. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

131. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

132. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate, contrary to Defendants' assertion that it has confirmed the security of its network. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

133. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure PII and PHI and to timely notify employees, patients or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and the common law; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure PII and PHI.

134. This Court also should issue corresponding prospective injunctive relief requiring Defendants to, at minimum 1) disclose, expeditiously, the full nature of the Data Breach and the

types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of Plaintiff and Class members' PII and PHI possessed by Defendants; and 3) provide, at their own expense, all impacted victims with lifetime identity theft protection services.

135. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

136. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

137. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, pray for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: July 12, 2024

Respectfully Submitted,

ANAPOL WEISS

BY: RICHARD M. GOLOMB, ESQ.
MIRIAM BENTON BARISH, ESQ.
KEVIN FAY, ESQ.
ROBERT G. DEVINE, JR., ESQ.
Identification Nos.: 42845, 72622, 308252, 327833
One Logan Square
130 N. 18th Street, #1600
Philadelphia, Pennsylvania 19103
Telephone: (215) 790-4571
rgolomb@anapolweiss.com
mbarish@anapolweiss.com
kfay@anapolweiss.com
bdevine@anapolweiss.com